UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,164	10/25/2001	Thomas S. Messerges	CR00287M	3410

22917 7590 02/03/2006

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
ABYANEH, ALI S	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,164	MESSERGES ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-25 are presented for examination.

Response to Arguments

2. The declaration filed on 11-14-2005 under 37 CFR 1.131 has been considered but is ineffective to overcome the Bolosky reference (US Publication No 2002/0194484).

Insufficient evidence of Diligence Before References Date

The evidence submitted by applicant is insufficient to establish diligence from a date prior to the effective date of the Bolosky reference (March 21, 2001) to the US filing date of this application (Oct 25, 2001).

An applicant may be diligent within the meaning of the patent law when he or she is doing nothing, if his or her lack of activity is excused. Note, however, that the record must set forth an explanation or excuse for the inactivity; the USPTO or courts will not speculate on possible explanations for delay or inactivity. See In re Nelson, 420 F.2d 1079, 164 USPQ 458 (CCPA 1970).

The document submitted by applicant, as evidence for diligence does not provide supporting evidence indicating activities between March 21 2001 and Oct 25, 2001. In page 2 of the Declaration, item 1 and item 2, applicant indicated that, "in February 2001, the invention was submitted to the Motorola Patent committee" and "on Jun 22,2001 The Motorola Corporate Patent Committee decided to pursue this discloser", however there is a four months unexplained gap between Feb 2001 and Jun, 22, 2001 which

applicant has not provided any evidence of activities between this period, and furthermore, in page 2 of the Declaration, items 3 (asking for quotes), 4 (material needed to establish a quote), 5 (acceptance of the quote), and 6 (plane to review the hash table patent) does not show **any type of activity by the applicants** and does not establish sufficient diligence.

Claim Rejections - 35 USC § 112

3. Claims 17, 21 and 25 rejected under 35 U.S.C. 112, second paragraph, as being indefinite because they are directed to a decryption process in absence of encryption, in another word the claim limitation includes "decrypting the chunk" while it is not clear at what stage the encryption took place.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 9, 15, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Hanna et al. (International Publication NO WO 99/40702).

Regarding claim 1

Chan teaches a method of creating a signed content hash, comprising: a plurality of chunks of content ((column 3, lines 51-53)(examiner considers software components as applicant chunk of content)); hashing each chunk of the plurality of chunks of content into a hash table; and signing the hash table (column 4, lines 1-10). Chan does not explicitly teach **dividing content** into a plurality of chunks of content. However, in analogous art, Hanna teaches dividing content into a plurality of chunks of content (page 3, lines 15-17). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan to include Dividing the content into a plurality of chunks of content. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to protect and verify the data and furthermore to protect individual portions of the data and provide an easier method for recognizing a corruption (page 3, lines 10-11).

Regarding claim 9

Chan teaches a method of authenticating a content hash, comprising: authenticating a hash table containing a plurality of chunk hashes corresponding to a plurality of chunks of content (column 4, lines 13-20); authenticating each chunk of the plurality of chunks of content (column 4, lines 20-30)(examiner considers digests of software components as applicant's chunk hashes). Chan

does not explicitly teach **dividing content** into a plurality of chunks of content. However, in analogous art, Hanna teaches dividing content into a plurality of chunks of content (page 3, lines 15-17). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan to include Dividing the content into a plurality of chunks of content. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to protect and verify the data and furthermore to protect individual portions of the data and provide an easier method for recognizing a corruption (page 3, lines 10-11).

Regarding claim 2

Chan and Hanna teach all limitation of the claim as applied to claim 1 above. Chan furthermore teaches a method, wherein hashing each chunk of the plurality of chunks of content into the hash table comprises: calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes corresponding to the plurality of chunks of content; and storing the plurality of chunk hashes in the hash table (column 3, lines 48-53).

Regarding claim 3

Chan and Hanna teach all limitation of the claim as applied to claim 1 above. Chan furthermore teaches a method, wherein dividing the content into the

plurality of chunks of content and hashing each chunk of the plurality of chunks of content into the hash table is repeated a plurality of times to create a corresponding plurality of hash tables (column 4, lines 20-23).

Regarding claim 15

Chan and Hanna teach all limitation of the claim as applied to claim 9 above. Chan furthermore teaches a method, wherein authenticating each chunk of the plurality of chunks of content comprises: calculating a recalculated chunk hash of the chunk of content to provide a recalculated chunk hash corresponding to the chunk of content; comparing the recalculated chunk hash to the chunk hash of the chunk stored in the hash table; and if the recalculated chunk hash matches the chunk hash of the chunk stored in the hash table, verifying the authenticity of the chunk (column 4, lines 4-30).

Regarding claim 16

Chan and Hanna teach all limitation of the claim as applied to claim 15 above. Chan furthermore teaches a method, further comprising: processing the chunk of content by having the recalculated chunk hash of the chunk of content calculated concurrently with calculating the recalculated chunk hash of the chunk (column 4, lines 4-30).

Regarding claim 18

Chan and Hanna teach all limitation of the claim as applied to claim 9 above. Chan furthermore teaches a method, wherein dividing the content into the plurality of chunks of content and authenticating each chunk of the plurality of chunks of content is repeated a plurality of times to authenticate a corresponding plurality of hash tables (column 4, lines 20-30).

6. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Danieli (US Patent NO. 6,510,513).

Regarding claim 19

Chan teaches a method of authenticating digital content, comprising: calculating an overall hash of a hash table containing a plurality of chunk hashes corresponding to a plurality of chunks of content; comparing the hash of the hash table to a hash recovered from a digital signature; and if the overall hash of the hash table matches the hash of the digital signature, verifying the authenticity of the plurality of chunks of the content (column 4, lines 4-30). Chan does not explicitly teach comparing the overall hash of the hash table to **a hash contained in a certificate**; and if the overall hash of the hash table matches the **hash of the certificate**, verifying the authenticity of the plurality of chunks of the content. However, in an analogous art, Danieli teaches a method wherein a

computed hash is compared with a hash contained in the certificate (column 2, lines 58-65). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chan's method to include comparing the overall hash of the hash table to a hash contained in a certificate; and if the overall hash of the hash table matches the hash of the certificate, verifying the authenticity of the plurality of chunks of the content. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to guarantee the authenticity and validity of the data and furthermore to provide security services and policy enforcement for electronic data (column 2,lines 42-43).

Regarding claim 20

Chan and Danieli teach all limitation of the claim as applied to claim 19 above. Chan furthermore teaches a method, wherein verifying the authenticity of the plurality of chunks if the overall hash of the hash table matches the hash of the certificate, further comprises for each chunk of the plurality of chunks of content: calculating a hash of the chunk to create a chunk hash of the chunk; comparing the chunk hash to a stored chunk hash of the chunk stored in the hash table; and if the chunk hash matches the stored chunk hash, verifying the authenticity of the chunk (column 4, lines 4-30).

7. Claims 4-8, 10-14 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Hanna et al. (International Publication NO WO 99/40702) further in view of Danieli (US Patent NO. 6,510,513).

Regarding claim 22

Chan teaches a method of authenticating digital content, comprising: calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes stored in a hash table corresponding to the plurality of chunks of content (column3, lines 48-53); hashing the plurality of chunk hashes of the hash table to create an overall hash of the content of the content package; determining whether a recalculated overall hash of the hash table matches the overall hash of the hash table; if the recalculated hash of the hash table matches the overall hash of the hash table, verifying the authenticity of each chunk of the plurality of chunks of the content (column 4, lines 4-30). Chan does not explicitly teach **dividing content** of a content package into a plurality of chunks of content. However, in analogous art, Hanna teaches dividing content of a content package into a plurality of chunks of content (page 3, lines 15-17). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan to include Dividing the content into a plurality of chunks of content. This would have been obvious because person having ordinary skill in the art at the time the

invention was made would have been motivated to do so in order to protect and verify the data and furthermore to protect individual portions of the data and provide an easier method for recognizing a corruption (page 3, lines 10-11). Chan and Hanna do not explicitly teach **placing the overall hash into a certificate.** However, in an analogous art, Danieli teaches Placing (hash) digest into a certificate (paragraph 2, lines 61-62). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan and Hanna to place the overall hash into certificate. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to guarantee the authenticity and validity of the data and furthermore to provide security services and policy enforcement for electronic data (column 2,lines 42-43).

Regarding Claims 4, 5 and 6

Chan and Hanna teach all limitation of the claim as applied to claim 1 above. Chan furthermore teaches hash table in its entirety and an overall hash of the hash table (column 3, lines 48-53 and column 4, lines 1-7). Chan and Hanna do not explicitly teach, wherein signing the hash table comprises: **creating a certificate of authenticity** of the hash table; **signing the certificate of authenticity of the hash table** and wherein **the certificate of authenticity of the hash table** comprises the hash table in its entirety and comprises an overall

hash of the hash table. However, in an analogous art, Danieli teaches a method of certificate of authenticity of the hash and signing the certificate of authenticity of the hash (column 2, lines 45-57). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chan's and Hamma's method to include certificate of authenticity of the hash table; signing the certificate of authenticity of the hash table and certificate of authenticity of the hash table comprising the hash table in its entirety and an overall hash of the hash table. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to guarantee the authenticity and validity of the data and furthermore to provide security services and policy enforcement for electronic data (column 2,lines 42-43).

Regarding claim 7

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 6 above. Chan furthermore teaches a method, wherein creating the overall hash of the hash table comprises: hashing the plurality of chunk hashes stored in the hash table to create the overall hash of the hash table (column3, lines 48-53).

Regarding claim 8

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 4 above. Danieli furthermore teaches a method, wherein the certificate of

authenticity of the hash table comprises additional information relating to the content and a set of rules governing the use of the content (column 3, lines 6-9).

Regarding claim 10

Chan and Hanna teach all limitation of the claim as applied to claim 9 above but they do not explicitly teach a method, wherein authenticating the hash table comprises: verifying a certificate of authenticity of the hash table; and if the certificate of authenticity of the hash table is verified, authenticating the hash table. (column 2, lines 61-65). However, in an analogous art, Danieli teaches verifying a certificate of authenticity of the hash and authenticating if the certificate of authenticity of the hash is verified (column 2, lines 61-65). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Chan's and Hanna's method to include verifying a certificate of authenticity of the hash table; and if the certificate of authenticity of the hash table is verified, authenticating the hash table. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to guarantee the authenticity and validity of the data and furthermore to provide security services and policy enforcement for electronic data (column 2,lines 42-43).

Regarding claim 11

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 10 above. Chan furthermore teaches, verifying the certificate of authenticity of the hash table comprises: verifying a signature of the certificate of authenticity comprising the hash table in its entirety; and if the signature of the certificate of authenticity containing the hash table in its entirety is verified, verifying the authenticity of the hash table (column 4, lines 5-10).

Regarding claim 12

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 10 above. Chan furthermore teaches a method, wherein verifying the certificate of authenticity of the hash table comprises: verifying a signature of the certificate of authenticity comprising an overall hash of the hash table; calculating a recalculated overall hash of the hash table; and if the recalculated overall hash of the hash table matches the overall hash of the hash table, verifying the authenticity of the hash table (column 4, lines 4-30).

Regarding claim 13

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 12 above. Chan furthermore teaches a method, wherein calculating the recalculated overall hash of the hash table comprises: hashing the plurality of chunk hashes stored in the hash table to create the recalculated overall hash of

the hash table (column 4, lines 20-30).

Regarding claim 14

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 10 above. Danieli furthermore teaches a method, wherein verifying the certificate of authenticity of the hash table further comprises: verifying additional information in the certificate of authenticity of the hash table relating to the content and a set of rules governing the use of the content (column3, lines 6-9).

Regarding claim 23

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 22 above. Chan furthermore teaches a method, wherein determining whether the recalculated overall hash of the hash table matches the overall hash of the hash table comprises: recalculating the overall hash of the hash table to create the recalculated overall hash; comparing the recalculated overall hash to the overall hash; and if the recalculated overall hash matches the overall hash and a signature on the certificate is valid, verifying authenticity of the hash table (column 4, lines 4-30).

Regarding claim 24

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 22 above. Chan furthermore teaches a method, wherein verifying the

authenticity of each chunk of the plurality of chunks comprises for each chunk: recalculating a hash of the chunk to create a recalculated chunk hash of the chunk; comparing the recalculated chunk hash to the chunk hash of the chunk; and if the recalculated chunk hash matches the chunk hash of the chunk, verifying the authenticity of the chunk (column 4, lines 4-30).

8. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Hanna et al. (International Publication NO WO 99/40702) further in view of Blaze (US Patent NO. 5,696,823).

Regarding claim 17

Chan and Hanna teach all limitation of the claim as applied to claim 16 above. Chan and Hanna do not explicitly teach a method, wherein processing the chunk of content further comprises: decrypting the chunk of content; and rendering the chunk of content to the user. However, in an analogous art, Blaze teaches decrypting the chunk of content and rendering the chunk of content to the user (column 4, lines 54-66). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan and Hanna to include decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package. This would have been obvious because person having ordinary skill in the art at the time the invention was

made would have been motivated to do so in order to enable the user to use the content and furthermore to derive the intermediate sub-block I1 (column 4, lines 62-65).

9. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Danieli (US Patent NO. 6,510,513) further in view of Blaze (US Patent NO. 5,696,823).

Regarding claim 21

Chan and Danieli teach all limitation of the claim as applied to claim 20 above but they do not explicitly teach, decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package. However, in an analogous art, Blaze teaches decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package (column 4, lines 54-66). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan and Danieli to include decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to enable the user to use the

content and furthermore to derive the intermediate sub-block I1 (column 4, lines 62-65).

10. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al. (US Patent NO 6,748,538) in view of Hanna et al. (International Publication NO WO 99/40702) in view of Danieli (US Patent NO. 6,510,513) further in view of Blaze (US Patent NO. 5,696,823).

Regarding claim 25

Chan, Hanna and Danieli teach all limitation of the claim as applied to claim 24 above but they do not explicitly teach a method, wherein contemporaneously with recalculating the hash of the chunk to create the recalculated chunk hash of the chunk, further comprising: decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package. However, in an analogous art, Blaze teaches decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package (column 4, lines 54-66). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method disclosed by Chan, Hanna, Danieli to include decrypting the chunk to provide a chunk of decrypted content of the content package; and rendering the chunk of decrypted content of the content package. This would

have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to enable the user to use the content and furthermore to derive the intermediate sub-block I1 (column 4, lines 62-65).

References Cited, Not Used

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Publication No. 2001/0032310

This reference relates to public key cryptosystems, and more particularly, to a public key validation service for validating a public key.

2. U.S. Patent No. 6,847,995

This reference relates to distributing project workloads among a distributed device and more particularly to techniques and related methods for managing, facilitating and implementing distributed processing in a network environment.

3. U.S. Patent No. 6,223,291

This reference relates to secure electronic commerce distribution and sales having the ability to offer software enhancements and new features in a simpler, faster and cheaper method.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Ali Abyaneh A.A
Patent Examiner
Art Unit 2137
01/18/2006